Data security - Four steps closer to GDPR & NDBs compliance for Law Firms

With the General Data Protect Regulation (GDPR) & Notifiable Data Breach scheme (NDBs) coming into effect this year, and with the threat of stricter audits, law firms are under increased pressure when handling sensitive and confidential client data. These days, an attachment containing personal data sent to an unauthorised recipient could be costly:

- NDBs - Fines up to $1.8M for organisations with >$3 Million revenue
- GDPR - Up to 4% of your annual global turnover or €20 Million (whichever is greater)

It's a difficult path for the legal sector. First, firms need to understand the requirements of the new regulations and then understand what data they're responsible for. Next, they need to map the two and create policies that will comply with the updated legislation. These are significant tasks, and with being pulled by compliance on one side and operations on the other, legal firms are walking a tightrope that can only be taken one step at a time.

Here are four steps you can take that will work towards GDPR & NDBs compliance.

1. Clean metadata

Legal professionals are notoriously overworked and under intense time pressure. They’re emailing documents all the time and, with each document that’s sent, there’s the potential for the wrong piece of information to slip into the wrong hands.

You can help stop personnel from inadvertently sending sensitive or confidential data to the incorrect people by introducing metadata cleaning policies. Policies can be general or of a specific nature, factoring in types of metadata, like track changes, file properties, speaker notes, as well as where the email is going, like whether it’s being sent internally or externally.

2. Check email recipients

We all know how often attachments are sent to the incorrect email recipient, either inadvertently or maliciously. It's the number one cause of data loss for businesses. One significant step towards avoiding data leaking from your business in this way is to move to a pessimistic data sharing model.

To protect your firm, you can associate confidential attachments to a whitelist or blacklist of email recipients. For example, you can limit matter files belonging to certain clients to a limited subset of people who “need to know” information for each engagement.

Alternatively, you can secure certain engagements by blocking matter files from being sent to free email domains, such as Gmail, Hotmail and so on.

For the truly paranoid clients that some of you have, you can also block their matter attachments going out over email at all, collaborating over secure online file transfer instead.

3. Monitor data loss via email

Most law firms consider threats to be outward-facing and miss the threat from the behaviour and actions of their own employees. Suspicious behaviour could be a sign that staff are planning to leave a firm, or are about to violate a firm policy regarding data sharing. Keep a watchful eye on the behaviour of possible "errant employees" in your firm by using software that provides internal, individual threat assessment. With a complete risk assessment solution, a risk score is assigned by analysing behaviours of internal team members and then comparing them against past behaviours and the behaviours of their cohorts. Both the frequency of emails sent and the content of each email (number of attachments, variety of attachments) is taken into account. Security admins can then actively utilise this information to manually review individuals breaching a threshold.

4. Refine firm-wide email security policies

It’s a cycle of continual refinement.

At the beginning, your best judgement to create security policies is required. Once they’re in place, ongoing monitoring of your mail flow to detect any emails that are violating the rules you set is vital. With this information, you can refine security policies, making them more robust with each iteration.

If you’re unsure of where to start, you can introduce monitoring software first, watch for a little while and then use this information to create appropriate security policies.

When choosing monitoring software, look for reports that you find easy to read. Masses of data can be overwhelming but when it’s filtered and presented using specific industry insights, it truly becomes meaningful and valuable to your business.

Keep asking questions

We’re living in an interesting time for data security and we hear from a lot of people walking the fine line between complying with the GDPR &/or NDBs and keeping daily operations running smoothly.

If you’ve got questions, we’re happy to talk through your challenges to discover if we can provide more valuable information or assistance. We’d love to share knowledge of best practices that has been derived from working with the world’s leading law firms, as security truly is a collaborative effort.

For more details and information please contact:
go5plus office: 02 8379 6988
Nick Goldrick (m) 0414 407 770 (e) nick@go5plus.com

Disclaimer - This document does not constitute legal opinion and go5plus is not liable for any actions undertaken based on the information provided within.